Side Channel Attacks on STTRAM and Low-Overhead Countermeasures

Anirudh Iyengar and Swaroop Ghosh
School of Electrical Engineering and Computer Science
Pennsylvania State University
University Park, PA, USA, 16828

Abstract: *Spin-Torque Transfer RAM (STTRAM), although promising, suffers from high write latency and write current. Additionally, the latency and current depends on the polarity of the data being written. These factors introduce security vulnerabilities and expose the cache memory to side channel attacks. In this paper, we propose a side channel attack (SCA) model where the adversary can monitor the supply current of the memory array to partially identify the sensitive cache data that is being read or written. We propose solutions such as short retention STTRAM, obfuscation of SCA using 1-bit parity, multi-bit random write, and, neutralizing the SCA using constant current write driver to mitigate such attacks.*

Keywords: Side Channel Attack; Last Level Cache; STTRAM; Data Privacy; Magnetic Tunnel Junction.

Introduction

Spin-Torque Transfer RAM (STTRAM) [1] is a promising candidate for Last Level Cache (LLC)due numerous benefits such as high-density, non-volatility, high-speed, low-power and CMOS compatibility. Fig. 1 shows the STTRAM cell schematic with Magnetic Tunnel Junction (MTJ) as the storage element. The MTJ contains a free and a pinned magnetic layer. The resistance of the MTJ stack is high (low) if free layer magnetic orientation is anti-parallel (parallel) compared to the fixed layer. The MTJ can be toggled from parallel to anti-parallel (or vice versa) by injecting current from source-line to bitline (or vice versa). The data in MTJ is stored in the form of magnetization. The data stored is '1' if the free layer magnetization is anti-parallel to fixed layer magnetization and '0' if they are parallel. The read/write latency of MTJ depends on the size of the device, current passing through the layers as well as on process variation.

Although promising, STTRAM is vulnerable towards ambient parameters like magnetic field and temperature, which can be employed to tamper with the stored data. The free layer of MTJ flips under the influence of external magnetic field which can be exploited by the adversary to launch magnetic attacks using a horseshoe magnet or an electromagnet [2]. The switching of MTJ depends on the ambient temperature, at high temperature the MTJ resistance reduces resulting in high read and write current [3]. The increased read current leads to read disturb failures, where the bits are accidentally flipped during read operation. The temperature can also be exploited to extend the persistence of the memory [7]. The persistent user data in non-volatile cache can also be compromised by launching unauthorized read and write operation, and probing the data buses after the authentic user has logged off. The persistent data leaving the cache can also be accessed by probing the data bus between the cache and main memory [4].

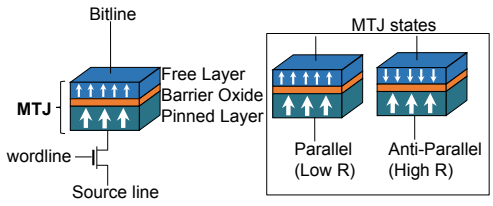

Fig. 1 Schematic of STTRAM bitcell showing MTJ.

Traditional cache attacks can also be extended for STTRAM such as, (a) micro-probing, where conductors are attached to the chip surface directly to interfere with the integrated circuit; (b) radiation imprinting, where the contents are burned in using X-Ray radiation to prevent overwriting or erasing of stored data; (c) optical probing, where a laser is shinned on the surface resulting in activating the underlying circuit. The active components glow, which can then be used to interpret the stored data.

In this work, we investigate the Simple Power Analysis (SPA) based SCA, to decipher the contents of the STTRAM LLC by monitoring the current drawn from the supply during read and write operations. The fact that STTRAM is associated with high write latency, high write current and asymmetry (polarity dependent) of writes, makes it vulnerable to SCA that can compromise data privacy and integrity. The current in a circuit can be measured by inserting a small resistance in series with the Vdd or ground rail and measuring the voltage drop across it. Sophisticated devices can be used to sample the voltages at high rates (1GHz) with excellent accuracy (< 1% error) [5]. The system level illustration of the die and the regulated power supply is shown in Fig. 2(a). Although on-chip regulators have been investigated, due to its limited presence in ICs makes SPA-based attacks non-trivial.

Fig. 2(d) shows the variation of supply current when a 512b word is written into the LLC. In order to mimic the power signature of a processor core, we implement 15, 17, 19 and 21-stage ring-oscillators and instantiate those 250 times. We note the change in the DC current level upon bit-flip from all-0 to all-1 which is a direct indication of the value of data being written.

STTRAM Vulnerabilities and Attack Models

A. Read/Write Latency:

The write latency of STTRAM is a function of thermal stability factor (Δ_t) and is susceptible to process variation (PV)

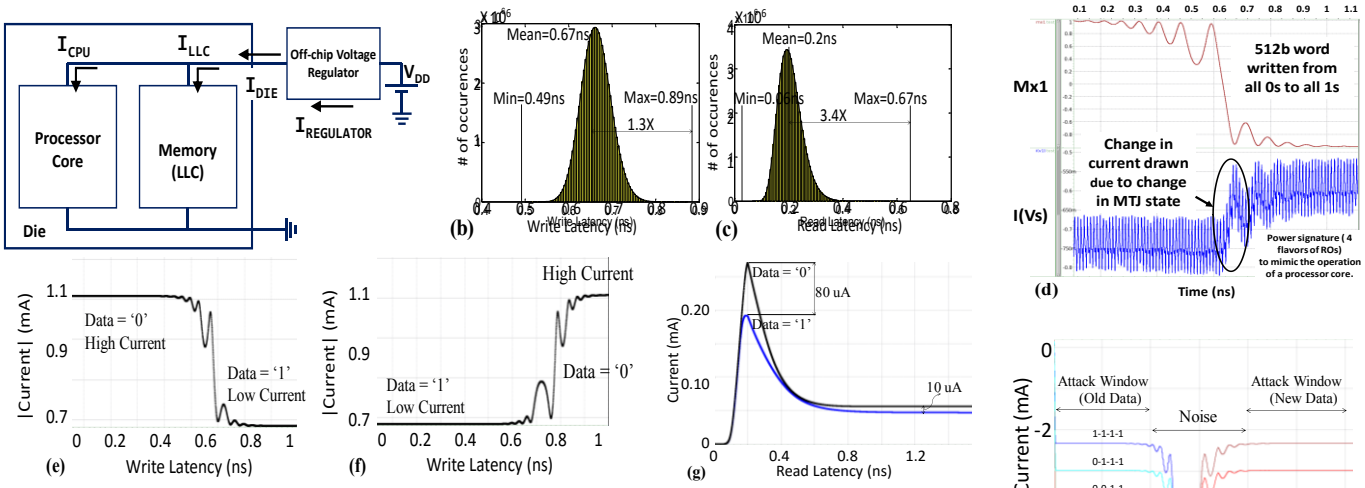

Fig. 2 (a) System level view comprising of CPU, LLC and external voltage regulator. (b) Write latency; (c) read latency distribution of an 8MB STTRAM cache under process variation. (d) Power signature of an example system consisting of 4 flavors of ring-oscillators (250 each) to mimic CPU along with a 512b word STTRAM LLC. (e) Supply current waveform (y-axis values are negative) for write '1'; (f) write '0', and (g) read operations

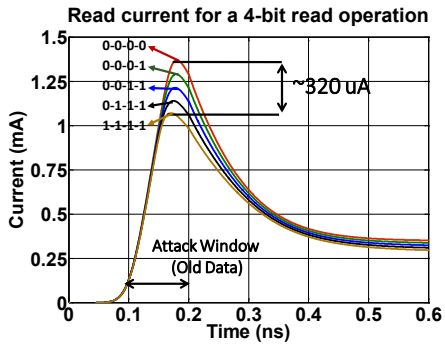

Fig. 3 Read currents for 4-bit read operation

[6], thus causing some bits to suffer from excessive high read and write latencies. Fig. 2(b-c) shows the read and write latency distribution of a 40nmx40nmx4nm STTRAM under PV. This high read and write latency provides a larger attack window to the adversary. By monitoring the current waveforms, the adversary can not only predict the number of 0's and 1's in the new data that is being written but can also predict the previous data by sampling the current just after the wordline is asserted. The adversary samples the current during the attack window shown in Fig. 2(h). Thus, data dependency of current reveals the stored and new data and higher latency facilitates the attack. Additionally, the attack window available to identify the old and new data. Furthermore, larger word size increases the total current which makes the attack easier for the adversary.

B. *Read/Write Current:*

STTRAM resistance is high (low) during state '1' ('0'). Fig. 2(e) shows the supply current waveform for single bit write '1' when the previous value stored is '0'. Initially the current is high (STTRAM resistance low) and it goes low after successful write. Fig. 2(f) shows the supply current waveform for write '0' with previous value stored as '1', in this case the current is initially low and goes high after successful write. The high and low states of current are very distinct and they reveal the information about the previous and new data. The read current is comparatively less than the write current (Fig. 2(g)), thus the read and write operation can be distinctly identified from the current waveforms. Fig. 2(h)/3 shows the write/read current waveforms for 4-bit write/read operation in STTRAM. Out of 16 data values only 5 are unique in terms of total number of 0's and 1's (1111, 0111, 0011, 0001, 0000). Knowing the number of 0's and 1's weakens the security significantly as it reduces the reverse engineering effort to identify the correct data.

C. *Temperature:*

The thermal stability (Δt) of STTRAM is a function of ambient temperature and the write current and write latency linearly depends on the thermal stability. The thermal stability is given by $\Delta_t = \frac{H_k M_s A_r t}{2 k_B T}$. where *Hk = uniaxial anisotropy, Ms= saturation magnetization, Ar= area of MTJ, t=thickness of free layer, kB= Boltzmann constant, T= ambient temperature.*

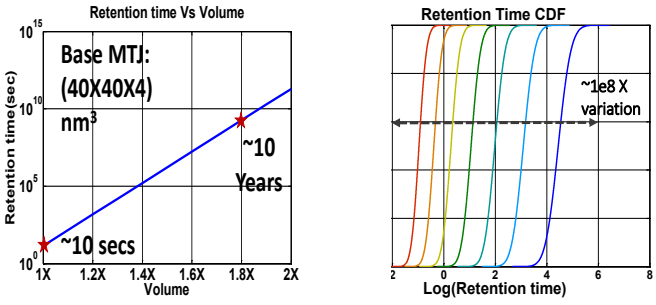

Fig. 4 (a) Retention time variation with respect to MTJ volume; and, (b) retention time dependence on temperature.

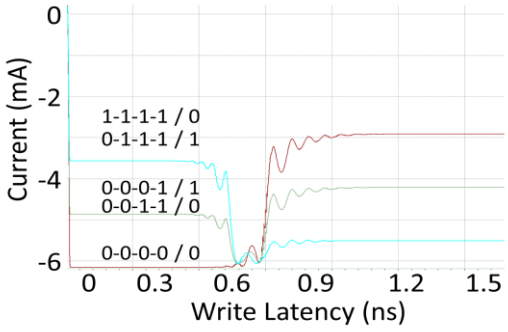

Fig. 5 Current waveform for 4-bit write with 1-bit parity.

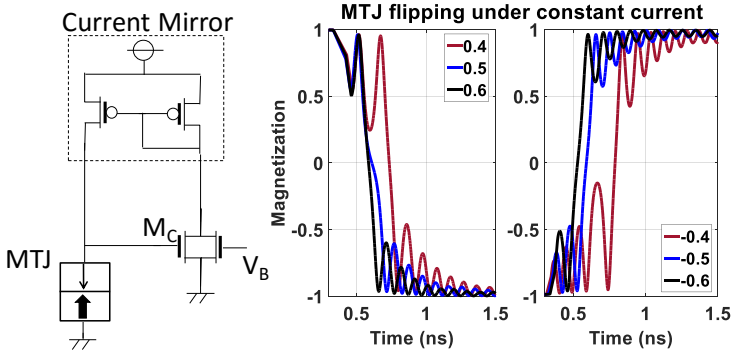

Fig. 6 (a) Constant current write circuit [8]; and, (b) write latency difference with constant current write (current in mA).

The write latency is directly proportional to the write current and thus at lower temperatures the write latency increases which provides adversary more time to launch the attack (Fig. 4(b)).

Prevention Techniques

Due to the predominantly strong supply current signature, we focus our efforts towards obfuscating the write operations.

A. Semi Non-Volatile Memory (SNVM):

SNVM is a non-volatile memory with lower retention time which can find potential use in cache application as the data is invalidated when the system restarts or the virtual address space is changed. The write latency and write current (I) linearly depends on the thermal barrier (Δ_t) of STTRAM. The retention time (t) is exponentially related to Δ_t by $t = C \times e^{k\Delta t}$, where C and k are fitting constants. We note that, both write latency and write current can be lowered by reducing the free layer volume of STTRAM (Fig. 4(a)).

B. Adding 1-bit parity:

The objective of this prevention technique is to merge multiple supply current levels in the side channel current waveform, which will make it difficult for the adversary to predict the states accurately. This is achieved by writing an extra parity bit along with the original data. Fig. 5 shows the current waveform of 4-bit write with 1-bit even parity. Therefore, instead of writing 4 bits we write 5 bits with the last bit value decided by the parity of the 4 bits. By doing this we can merge 5 states (Fig. 5) into 3 states. Compared to uncoded data the reverse engineering effort increases because a data will map to more number of possibilities.

C. Adding Random bits in Word:

To further obfuscate the signature, we propose to add multiple random bits in the word during write. This technique further complicates and merges the states in the supply current signature. For larger word sizes, the overhead from few extra bits is expected to be negligible.

D. Constant Current Write:

Constant current write can be achieved by using a current mirror with voltage controlled current source (Fig. 6(a)). The two PMOS forms the current mirror whereas the NMOS MC controls the current to be mirrored depending on the STTRAM resistance [8]. Bias voltage (VB) is adjusted to provide the initial read current in the main branch which will pass through the STTRAM in the auxiliary branch. However constant current write will create mismatch in switching times between '0' and '1' states (Fig. 6(b)). This will affect the design of the word-line driver but the adversary will have no clue about the data as the current will remain constant throughout the write access.

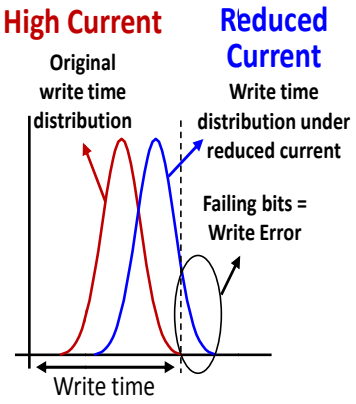

Fig. 7 Homogeneous write using reduced write current.

Reducing power overhead of constant current write: To ensure functional correctness, the constant current approach utilizes the worst case write current injected to homogenize the write current. This leads to power wastage while writing logic '1'. To address this issue, it is possible to leverage the trade-off that exists between write current and error rate (as shown in Fig. 7). By lowering the write current for both '0→1' and '1→0', the write-time of certain number of bits may fall beyond the worst latency. These bits contribute to the write error rate. By maintaining the write error rate under permissible levels or increasing the permissible write latency it is possible to lower the power overhead of constant current write.

Discussions

A. Impact of Scaling:

With technology scaling the MTJ size reduces which lowers the free layer thickness. The thermal stability (Δt) is linearly dependent on the free layer thickness and the retention time is exponentially related to Δt. There-fore, the write latency and write current of STTRAM is expected to scale down making it more secure against power analysis attack. Introduction of perpendicular magnetic anisotropy (PMA)

STTRAM makes it further challenging for the adversary to perform meaningful side channel attack due to inherently lower write latency and write current.

B. Impact of TMR:

As described earlier, the TMR ratio determines the resistance difference between the two MTJ states. It is therefore evident that, larger the TMR, greater will be the difference of resistance between the two MTJ states. For a good sense margin, a large TMR is always desired. How-ever, this can prove detrimental from a security point of view as it will allow a clearer distinction between the bits being written/read. Thus, improving the effectiveness of SPA.

C. Impact of Usage:

Although STTRAM LLC is considered in this paper the proposed attack models are equally applicable to the STTRAM main memory. Availability of dedicated power supply makes it easy to probe main memory active current. However, cryptographic keys cannot be revealed since the crypto operations are performed on chip. Nevertheless, the raw unencrypted sensitive data can be extracted.

D. Impact of Magnetic Tampering:

External DC magnetic field of opposite strength could be used to increase the switching time of MTJ, which will increase the attack window for the adversary. Thus, with the help of a common horseshoe magnet the adversary can increase the write latency to facilitate attacks (especially for constant voltage write).

E. Cache Timing Attack:

In shared computer, the main memory and hard disk are protected against use by another user on the same machine but the cache is not. If two users are working on the same machine, the malicious user can fill the entire cache with his own data and wait for the other user to perform secret operations like encryption. The malicious user then measures the loading time to find which of his data has been replaced by the other user and learns about the cache addresses used in encryption. This timing information can be exploited for key recovery of encryption algorithms like AES [9]. Since a larger cache size can be afforded with STTRAM (due to smaller footprint bitcell) the number of cache line replacements is expected to be less alleviating the cache timing attack. However, the persistence of data can be exploited to launch the attack at a later time to retrieve the sensitive information.

F. Other Side Channels:

STTRAM resistance in the parallel and anti-parallel state is in the range of KΩ (5K-10K) and the write current is in the order of μA (100-150 μA). Thus, the IR drop will be in the order of mV resulting in considerable droop in supply voltage. The adversary can monitor the droops in supply voltage to identify write operation and the amount of droop can give out the information about the data being written much like supply current.

G. Considerations for Other NVMs:

Long/asymmetric write latency and high/asymmetric write current is common challenge for other NVMs such as Resistive RAM, Phase Change RAM and Domain Wall Memory. Therefore, the attack models presented in this paper are equally applicable to the emerging NVMs. Due to generic nature of the solutions pro-posed in this paper; similar techniques could also be extended to other NVMs for mitigation.

Conclusions

In this paper, we showed that STTRAM read/write current, latency and asymmetricity can be security vulnerabilities. We presented novel SCA models for STTRAM to compromise the sensitive data in LLC. We also provided a suite of preventive countermeasures such as constant current write, increased word size, SNVM and parity bit encoding to increase the reverse engineering effort required by the adversary to decipher the data from read and write current waveforms. The proposed techniques showed significant promise to protect against data privacy attacks to enable secure NVM design. The solutions proposed in this paper could also be extended to other NVMs for attack mitigation.

Acknowledgements

This paper is based on work supported by Semiconductor Research Corporation (#2442.001) and National Science Foundation (CNS-1441757).

References

[1] Ohsawa, T et. al, "1Mb 4T-2MTJ nonvolatile STT-RAM for embedded memories using 32b fine-grained power gating technique with 1.0 ns/200ps wake-up/power-off times." In VLSIC, 2012 Symposium on, pp. 46-47. IEEE, 2012.

[2] Jang, Jae-Won et. al, "Self-correcting STTRAM under magnetic field attacks." DAC, 2015 52nd ACM/EDAC/IEEE, pp. 1-6. IEEE.

[3] Bi, Xiuyuan et. al, "Analysis and optimization of thermal effect on STT-RAM Based 3-D stacked cache design." In VLSI (ISVLSI), 2012 IEEE Computer Society Annual Symposium on, pp. 374-379. IEEE, 2012.

[4] Rathi, Nitin et. al, "Data Privacy in Non-Volatile Cache: Challenges, Attack Models and Solutions", In ASPDAC, IEEE, 2016.

[5] Jameco Electronics, "PC-Multiscope (part# 142834)," p.103, 1999.

[6] Motaman, Seyedhamidreza et. al, "Impact of process-variations in STTRAM and adaptive boosting for robustness." In Proceedings of the 2015 DATE, pp. 1431-1436. EDA Consortium, 2015.

[7] Haldermanet al, "Lest we remember: cold-boot attacks on encryption keys." Communications of the ACM 52, no. 5 (2009): 91-98.

[8] Halupka, David. "Effects of Silicon Variation on Nano-Scale Solid-State Memories." PhD diss., University of Toronto, 2011.

[9] Bernstein, Daniel J. "Cache-timing attacks on AES." (2005).